UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

IN RE: MOVEIT CUSTOMER DATA SECURITY BREACH LITIGATION	MDL No. 1:23-md-03083-ADB-PGL
This Document Relates To: 1:23-cv-12478 1:23-cv-12281 1:23-cv-12561 1:23-cv-13079 1:24-cv-11523 1:23-cv-12226 1:23-cv-12273	

DECLARATION OF GARY F. LYNCH IN SUPPORT OF PLAINTIFFS' MOTION FOR PRELIMINARY APPROVAL

I, Gary F. Lynch, pursuant to 28 U.S.C. § 1746, declare as follows:

1. I am an attorney licensed in Pennsylvania and New York and have been admitted to practice before the Supreme Court of the United States and numerous federal appellate and district courts. I have been appointed by this Court to serve as Co-Lead Counsel for MDL Plaintiffs. I have been active in all aspects of this Litigation. I submit this Declaration in support of Plaintiffs' Unopposed Motion for Preliminary Approval of Proposed Class Action Settlement (the "Declaration"). The information set forth in this Declaration is based upon my personal knowledge.

2. I am a founding member of the law firm of Lynch Carpenter, LLP ("Lynch Carpenter" or the "Firm") and have been engaged in the practice of law for over thirty years, with the majority of my career spent representing plaintiffs in the litigation of complex civil cases and class actions. The primary focus of my practice is data breach and data privacy litigation.

3. I have spent the bulk of my professional time representing individual and institutional plaintiffs in class action and multi-district litigation throughout the country and am currently serving, or have served, as lead or co-lead counsel in numerous federal and state class actions and multidistrict proceedings, including, among others: *In re Wawa, Inc. Data Sec. Litig.*, No. 19-cv-6019 (E.D. Pa) (appointed co-lead of consolidated data breach on behalf of financial institution plaintiffs and reached a $37 million settlement for the financial institution class, as mediated by former Magistrate Judge Diane Welsh; final approval pending); *In re Equifax, Inc., Customer Data Sec. Breach Litig.*, No. 1:17-md-02800 (N.D. Ga.) (appointed co-lead MDL counsel on behalf of financial institution plaintiffs and reached a $7.75 million settlement for the financial institution class); *In re Home Depot Data Breach Litig.*, No. 1:14-md-2583 (N.D. Ga.) (same and $27 million settlement for the financial institution class); *First Choice Fed. Credit Union v. The Wendy's Co*., No. 2:16-cv-00506 (W.D. Pa.) ($50 million settlement for the financial institution class); *Dittman v. UPMC d/b/a The Univ. of Pittsburgh Med. Ctr.*, No. GD-14-003285 (Pa. Ct. Com. Pl.) (lead counsel on behalf of plaintiffs after obtaining reversal in the Pennsylvania Supreme Court).

4. In addition to serving as lead counsel in major data breach litigation, I have also served in leadership committee positions in many other data breach/privacy cases, including: *In re Target Corp. Customer Data Sec. Breach Litig.*, MDL No. 2522 (D. Minn.) (appointed to the Executive Committee managing the litigation on behalf of all plaintiffs [consumers, financial institution, and shareholders]. The case ultimately settled for $10 million [for consumers] and $39 million [for financial institutions]); *In re Marriott Int'l Customer Data Sec. Breach Litig.*, MDL No. 2879 (D. Md.); *In re: Cmty. Health Sys., Inc*., *Customer Sec. Data Breach Liti*g., MDL No. 2595, 15-cv-0222 (N.D. Ala.); *In re: Arby's Rest. Grp., Inc. Data Sec. Litig*., No. 17-mi-55555

(N.D. Ga.); *Greater Chautauqua Fed. Credit Union et al v. Kmart Corp*., No. 15-cv-02228 (N.D. Ill.); *In re Vizio, Inc. Consumer Priv. Litig*., MDL No. 2693 (C.D. Cal.) (consumer privacy breach, steering committee; $17 million settlement).

5. I make this Declaration in support of the proposed Class Settlement Agreement and Release ("Settlement") reached between the Plaintiffs[1] and Defendant Nuance Communications, Inc. ("Nuance" or "Defendant") after extensive arm's-length negotiation, a true and accurate copy of which is being filed concurrently herewith. Based upon my experience serving as lead counsel and other leadership positions in class action litigation, it is my opinion that the proposed Settlement in this Litigation[2] is fair, adequate, and reasonable, so as to satisfy the requirements for preliminary and, ultimately, final approval pursuant to Fed. R. Civ. P. 23. This opinion is shared by Court-appointed Co-Lead Counsel, E. Michelle Drake, Douglas McNamara, Karen Riebel, and Charles Schaffer, Coordinating & Liaison Counsel, Kristen A. Johnson, and the members of the Settlement Committee, Brian Gudmundson, Jonathan Jagher, Norman Siegel, and Courtney Maccarone, all of whom played a role in negotiating and finalizing the Settlement.

BACKGROUND ON THE SECURITY INCIDENT

6. The Settlement resolves claims asserted against Nuance (and Nuance Clients who provided data to Nuance) for harms that resulted from Nuance's use of MOVEit Transfer, a file transfer tool created by Progress Software Corporation ("Progress").

7. MOVEit Transfer is a subscription-based managed file transfer software licensed by Progress and used by numerous commercial entities and federal and state agencies, including Nuance.

[1] Plaintiffs are Denise Peel, Kristen Eyester, Juan Salas, Patricia Callahan, Kayla Farrar, and Justin Okeke ("Plaintiffs" or "Settlement Class Representatives").
[2] Capitalized terms, unless otherwise defined, adopt the definitions from the Settlement.

8. Between May 27, 2023, and May 31, 2023, CL0P Ransomware Gang identified and exploited a vulnerability in MOVEit Transfer that allowed them to access the data contained therein (the "MOVEit Security Incident"). CL0P used the MOVEit vulnerability to escalate user privileges, gain unauthorized access to customer environments, and access, copy, and exfiltrate the sensitive information stored there. Progress later warned that an unauthenticated SQL vulnerability could allow unauthorized actors to escalate privileges and access users' MOVEit environments.

9. According to Nuance's notice of the Security Incident, the Security Incident resulted in the theft of information from Nuance's MOVEit environment.

10. After Progress informed Nuance of the vulnerability in MOVEit Transfer, Nuance performed an investigation into the Security Incident. Its investigation determined that individuals' Personal Information had been taken from its MOVEit environment due to an exploit of the MOVEit vulnerability. The stolen information included Settlement Class Members' Personal Information exchanged with Nuance by its downstream data custodians, including healthcare organizations using Nuance's services.

11. Nuance determined that approximately 1.225 million Settlement Class Members had their Personal Information impacted due to Nuance's use of MOVEit Transfer. On or around September 22, 2023, Nuance began issuing individual notices of the incident.

12. Plaintiffs are individuals whose Personal Information was impacted by Nuance's use of MOVEit Transfer. Plaintiffs received data breach notices from Nuance informing them that their Personal Information had been impacted in the Security Incident. After receiving notices from Nuance, Plaintiffs filed actions against a combination of Nuance and Progress related to the Security Incident in the United States District Court for the District of Massachusetts. *See Callahan v. Nuance Commc'ns, Inc.*, No. 23-cv-12478 (D. Mass.); *Eyester v. Nuance Commc'ns., Inc.*, No.

23-cv-12281 (D. Mass.); *Farrar v. Nuance Commc'ns, Inc.*, No. 23-cv-12561 (D. Mass.); *Markley v. Nuance Commc'ns, Inc.*, No. 23-cv-13079 (D. Mass.); *Okeke v. Progress Software Corp.*, No. 24-cv-11523 (D. Mass.); *Peel v. Nuance Commc'n's, Inc.*, No. 23-cv-12226 (D. Mass.); and *Salas v. Nuance Commc'ns, Inc.*, No. 23-cv-12273 (D. Mass.). Two additional actions were also filed against Nuance, which have since been voluntarily dismissed: *Johnson v. Nuance Commcn's, Inc.*, No. 23-cv-12265 (D. Mass.) and *Moore v. Nuance Commcn's, Inc.*, No. 23-cv-12446 (D. Mass.).

13. Plaintiffs' actions were then transferred to and coordinated with *In re: MOVEit Customer Data Sec. Breach Litig.*, MDL No. 1:23-md-03083-ADB, pending in the U.S. District Court for the District of Massachusetts before the Honorable Allison D. Burroughs.

14. On January 19, 2024, the Court appointed myself and several additional attorneys, E. Michelle Drake, Douglas McNamara, Karen Riebel and Charles Schaffer, as Co-Lead Counsel for all plaintiffs who filed actions consolidated in the MDL. The Court also appointed Kristen A. Johnson as Coordinating & Liaison Counsel, and Brian Gudmundson, Jonathan Jagher, and Norman Siegel as members of the Settlement Committee.

MEDIATION AND SUBSEQUENT NEGOTIATIONS

15. Lead Counsel, the Settlement Committee, and counsel for Nuance agreed to mediate the claims asserted against Nuance at an early point in the bellwether phase of this MDL in order to attempt to avoid the time and expense of litigation.

16. The parties agreed to mediate with Hon. Diane M. Welsh (Ret.), who mediated several other cases in the *MOVEit* MDL, two of which have separately settled.

17. Prior to mediation, the parties engaged in informal discovery, in which the parties propounded certain information requests and exchanged extensive information about Security Incident, including information concerning Nuance's use of MOVEit Transfer, the types of

information Nuance exchanged via MOVEit Transfer, the cause and scope of the breach, the number of individuals impacted, and the types of information taken. This information was reviewed by the Settlement Committee and myself and provided Lead Counsel and the Settlement Committee with the information needed to objectively evaluate the strengths and weaknesses of Plaintiffs' and Settlement Class Members' claims.

18. On January 28, 2025, the parties engaged in a full-day mediation session before Judge Welsh. The good-faith, hard-fought negotiations were successful, resulting in an agreement in principle.

19. Following the mediation, the parties engaged in a series of further arm's-length discussions as the parties continued to negotiate, draft, and finalize the terms of the Settlement Agreement. The finalized Settlement Agreement was fully executed as of July 25, 2025.

THE SETTLEMENT AGREEMENT PROVIDES SIGNIFICANT BENEFITS TO THE SETTLEMENT CLASS

20. The Settlement resolves claims asserted against Nuance (and Nuance Clients who provided data to Nuance) concerning the Security Incident. It does not resolve claims against Progress.

21. Under the Settlement Agreement, Nuance agreed to pay $8.5 million into a non-reversionary Settlement Fund to resolve Plaintiffs' and Settlement Class Members' claims against Nuance. The Settlement Fund will pay for: (1) costs of Notice and Settlement Administration; (2) any Service Awards for the Settlement Class Representatives approved by the Court; (3) any attorneys' fees and expenses approved by the Court; and (4) Settlement Payments for the Settlement Class pursuant to the Settlement and the Settlement Benefits Plan, as approved by the Court.

22. The Settlement provides relief to those whose Personal Information was provided to Nuance and subsequently compromised in the Security Incident.

23. The "Settlement Class" includes "all persons in the United States whose Personal Information was included in the files affected by the Security Incident." The "Security Incident" means "the exploitation of the MOVEit Transfer Software vulnerability on or around May 2023 that impacted thousands of entities that used the software, including Nuance, but, for purposes of this Agreement, only to the extent it impacted Nuance and Nuance Clients."

24. The Settlement requires that the Net Settlement Fund (after deducting for notice and administration costs and any Court-approved Service Awards to the Settlement Class Representatives and attorneys' fees and expenses) be distributed via a Settlement Benefits Plan proposed by Lead Counsel and the Settlement Committee.

25. Lead Counsel, with the assistance of the Settlement Committee, designed the Settlement Benefits Plan to provide Settlement Class Members with relief aimed at the heart of the harm caused by a data breach—out-of-pocket losses due to fraud, identity theft, or other harm resulting from the data breach; compensation for lost time spent responding to the Security Incident; credit monitoring and identity theft protection services; and an alternative cash payment to compensate Settlement Class Members for harm caused without having to provide documentation of any out-of-pocket losses.

26. Specifically, Settlement Class Members may submit a claim for one or more of the following:

a. Reimbursement of Ordinary Losses. Settlement Class Members will be able to submit a claim for reimbursement of unreimbursed losses, up to a total of Two

Thousand Five Hundred United States Dollars ($2,500.00) per Settlement Class Member. Such Ordinary Losses include:

i. Out-of-pocket expenses incurred as a result of the Security Incident (to be determined by the Settlement Administrator with no right of appeal), including bank fees, long distance phone calls, cell phone charges (only if charged by the minute), data charges (only if based on the amount of data used), postage, or gasoline for local travel;

ii. Fees for credit reports, credit monitoring, or other identity theft insurance products purchased between May 31, 2023 and the date of the close of the Claims Period; and

iii. Reimbursement for up to four (4) hours of lost time, at Twenty-Five United States Dollars ($25.00) per hour (up to $100.00 total), for time spent dealing with the Security Incident. Settlement Class Members must attest to the accuracy of any request for compensation for lost time.

b. Reimbursement of Extraordinary Losses. Settlement Class Members may submit a claim for up to Ten Thousand United States Dollars ($10,000.00) in compensation for proven monetary losses, professional fees (*e.g.*, attorneys' fees and accountants' fees), and fees for credit repair services as a result of the Security Incident ("Reimbursement of Extraordinary Losses"), provided that:

i. The loss is an actual, documented, and unreimbursed monetary loss;

ii. The loss was more likely than not caused by the Security Incident;

iii. The loss occurred between May 31, 2023, and the close of the Claims Period; and

iv. The loss is not covered by one or more of the Reimbursement for Ordinary Losses categories.

c. Alternative Cash Payment. In lieu of claiming compensation under Sections 6.2(a) and (b), Settlement Class Members may elect to receive a one-time payment of One Hundred United States Dollars ($100.00) (subject to a *pro rata* reduction or increase pending total claim submission) without the need to document losses or attest to time spent as a result of the Security Incident.

d. Credit Monitoring and Identity Theft Protection Services. Settlement Class Members may also elect to enroll in two (2) years of medical and credit monitoring services that will include, among other services: (a) healthcare insurance plan ID monitoring that tracks and alerts when a plan ID is exposed on the dark web; (b) Medical Record Number (MRN) monitoring that alerts when a medical record number is detected on the dark web; (c) National Provider Identifier (NPI) monitoring to track and alert when registered licensing credentials are found on the dark web; (d) Medicare Beneficiary Identifier (MBI) that alerts when MBI has been disclosed on the dark web; (e) International Classification of Diseases (ICD) monitoring, which notifies when an ICD Code is detected on the dark web; (f) health savings account monitoring, which monitors registered health savings accounts for unusual or unauthorized transactions; and (g) $1 million of medical identity theft insurance with no deductible. Settlement Class Members who elect to enroll in medical monitoring services will also receive two (2) years of one bureau credit monitoring. These services will be made available to all Settlement Class Members who choose to enroll regardless of whether they submit a claim for

Reimbursement of Ordinary Losses, Reimbursement of Extraordinary Losses, or an Alternative Cash Payment.

27. The reimbursement of out-of-pocket ordinary and extraordinary losses are intended to provide relief for costs commonly incurred due to data breaches, including unreimbursed fraud, telephone or cell phone charges, internet usage charges, credit monitoring, costs of credit reports, and bank or financial institution charges.

28. The reimbursement for lost time (as included in Reimbursement for Ordinary Losses), similarly, is intended to provide relief for time incurred responding to the Security Incident, including, for example, monitoring accounts, even if those actions did not cause an out-of-pocket loss.

29. The Alternative Cash Payment is intended to compensate Settlement Class Members for harm caused without having to provide documentation of any out-of-pocket losses.

30. Finally, the credit monitoring and identity theft protection services are intended to prevent harm from the future misuse of the impacted data, a risk all Settlement Class Members face due to having their Personal Information stolen.

31. If the total value of all Approved Claims exceeds the Net Settlement Fund available for distribution to Settlement Class Members, the Settlement Administrator shall reduce the *pro rata* value of Alternative Cash Payments to the highest amount that will allow all Approved Claims to be paid using the Net Settlement Fund available.

32. To the extent that there are any remaining monies in the Net Settlement Fund one-hundred eighty (180) days after the Effective Date, such monies will be used to extend the credit monitoring and identity theft services (for Settlement Class Members who filed Approved Claims

for that benefit) for as long as possible, until the Net Settlement Fund is completely exhausted. No funds may revert back to Nuance.

THE NOTICE PLAN IS THE BEST PRACTICABLE

33. The Settlement proposes a Notice Plan requiring direct notice to be emailed or, alternatively, mailed to each Settlement Class Member. The Settlement Administrator, A.B. Data, Ltd. ("A.B. Data") will be responsible for issuing notice according to the Settlement's terms.

34. Under the Settlement, Nuance will provide a list of Settlement Class Members within ten (10) days after the entry of an order preliminarily approving the Settlement. A.B. Data will undergo efforts to update the Settlement Class list to ensure accurate addresses.

35. For the purposes of effectuating individualized, direct Notice, A.B. Data shall send Short Form Notice with pertinent information regarding the Settlement Agreement via email when available, and via U.S. mail address where no email address is available.

36. The Settlement Administrator shall also establish a Settlement Website, which will include the Settlement Agreement, relevant pleadings, the Long Form Notice, any relevant Court orders regarding the Settlement, and a list of frequently asked questions mutually agreed upon by the Parties. The Long Form Class Notice describes plainly: (1) the allegations asserted in the Litigation; (2) details of the Settlement's benefits; (3) how to file a claim; (4) how Settlement Class Members can exclude themselves from the Settlement or object to the Settlement; (5) how to access the Settlement Website; and (6) contact information to learn more about the Settlement or answer any questions about filing a claim, submitting an objection, or opting out. The Notice Plan is consistent with other effective, court-approved settlement notice programs, including those involving data breaches, and is the best notice practicable. Under the Notice Plan, the parties expect virtually all Settlement Class Members to receive direct notice and will engage in other means if

it becomes apparent that some Settlement Class Members have not received notice. I believe the proposed Notice Plan represents the best practicable notice to Settlement Class Members and satisfies all due process considerations and meets the requirements of Federal Rule of Civil Procedure 23(e)(1)(b).

REQUEST FOR SERVICE AWARD AND ATTORNEYS' FEES AND EXPENSES

37. Under the Settlement Agreement, Lead Counsel may move the Court for award of attorneys' fees and expenses as a percentage of the fund and for payment of Service Awards to each of the Settlement Class Representative in the amount of $2,500.00.

38. Any amount awarded by the Court for the Service Awards and attorneys' fees and expenses will be paid from the Settlement Fund.

39. The Settlement is not contingent on the Court's approval of the payment of any attorneys' fees or expenses.

THE SETTLEMENT IS FAIR, REASONABLE, AND ADEQUATE

40. Lead Counsel and the Settlement Committee have reviewed the proposed Claim Form and the Notices to be used in the Settlement. The Claim Form is simple and straightforward and requires only the provision of very basic information. Based upon our experience with the settlement of other class action data breach cases on behalf of financial institutions and consumers, Lead Counsel believe that the simplicity of the Claim Form will increase participation from Settlement Class Members.

41. Lead Counsel and the attorneys on the Settlement Committee have experience litigating complex civil cases and class actions and have demonstrated particular success in litigating data security breach class actions. Lead Counsel and the Settlement Committee have vigorously pursued the Litigation and represented the interests of Plaintiffs and the Settlement

Class, and have a strong understanding of the strengths and weaknesses of Plaintiffs' claims based on their experience, knowledge obtained from representing Plaintiffs in the MDL, the exchange of information related to the Security Incident, and their vigorous mediation efforts. Lead Counsel and the Settlement Committee, thus, have adequate information to assess the reasonableness of the Settlement.

42. Based on our experience and expertise, Lead Counsel and the Settlement Committee believe that the settlement is fair, adequate, reasonable, an excellent result for the Settlement Class, and represents a desirable resolution of this Litigation. Generally speaking, there are many impediments to victory for victims of a data breach pursuing litigation, as well as significant impediments to class certification. In this case, all these uncertainties and impediments are present, as well as the additional issue presented by the fact that this data breach occurred as part of a much larger data breach involving Progress and its MOVEit software, which was used by hundreds of businesses impacted by the Security Incident.

43. Given these litigation risks, this Settlement is an excellent result in a complex, high-risk, hard-fought case that provides a substantial recovery for Plaintiffs and the Settlement Class who face significant future risk and, for some, have already experienced harm due to the Security Incident.

44. Because the Settlement represents a fair and reasonable recovery on behalf of Plaintiffs and the proposed Settlement Class, Lead Counsel and the Settlement Committee believe that the Court should preliminarily approve the Settlement and direct Notice to be issued to the Settlement Class.

45. Attached to this Declaration as Exhibit 1 is a true and correct copy of the Class Action Settlement Agreement and Release, including the Settlement's exhibits as follows:

a. Exhibit A: a copy of the proposed Claim Form;

b. Exhibit B: a copy of the proposed Final Approval Order and Judgment;

c. Exhibit C: a copy of the proposed Order of Preliminary Approval;

d. Exhibit D: a copy of the proposed Settlement Benefits Plan;

e. Exhibit E: a copy of the proposed Short Form Notice;

f. Exhibit F: a copy of the proposed Long Form Notice; and

g. Exhibit G: a copy of the proposed Reminder Notice.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on July 30, 2025.

/s/ Gary F. Lynch
Gary F. Lynch

CERTIFICATE OF SERVICE

I hereby certify that, on this date, the foregoing document was filed electronically via the Court's CM/ECF system, which will send notice of the filing to all counsel of record.

Dated: July 30, 2025

/s/ Kristen A. Johnson
Kristen A. Johnson (BBO# 667261)